EXHIBIT A

Commenters explained that the CDPA contains such a provision.[31]

One commenter suggested that a financial institution should only provide notice in response to inquiries. By contrast, other commenters stated that the final Guidance should make clear that general notice on a Web site is inadequate and that financial institutions should provide individual notice to customers.

The Agencies determined that the provision in the proposed Guidance that notice be delivered in a ''timely, clear, and conspicuous'' manner already appears elsewhere in the Guidance and does not relate to manner of delivery. This phrase appears elsewhere in the final Guidance and is unnecessary here.

The Agencies have decided not to include a provision in the final Guidance that permits notice through a posting on the Web or through the media in order to provide notice to a specific number of customers or where the cost of notice to individual customers would exceed a specific dollar amount. The Agencies believe that the thresholds suggested by commenters would not be appropriate in every case, especially in connection with incidents involving smaller institutions.

Therefore, the final Guidance states that customer notice should be delivered in any manner that is designed to ensure that a customer can reasonably be expected to receive it. This standard places the responsibility on the financial institution to select a method to deliver notice that is designed to ensure that a customer is likely to receive notice.

The final Guidance also provides examples of proper delivery noting that an institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive electronic communications from the institution.

Some commenters questioned the effect of other laws on the proposed Guidance. A few commenters noted that electronic notice should conform to the requirements of the Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C. 7001 *et seq.*

The final Guidance does not discuss a financial institution's obligations under the E-Sign Act. The Agencies note that the final Guidance specifically contemplates that a financial institution may give notice electronically or by telephone. There is no requirement that notice be provided in writing. Therefore, the final Guidance does not trigger any consent requirements under the E-Sign Act.[32]

Still other commenters requested clarification that a telephone call made to a customer for purposes of complying with the final Guidance is for ''emergency purposes'' under the Telephone Consumer Protection Act, 47 U.S.C. 227 (TCPA). These commenters noted that this is important because under the TCPA and its implementing regulation,[33] it is unlawful to initiate a telephone call to any residential phone line using an artificial or prerecorded voice to deliver a message, without the prior express consent of the called party, unless such call is for ''emergency purposes.''

The final Guidance does not address the TCPA, because the TCPA is interpreted by the Federal Communications Commission (FCC), and the FCC has not yet taken a position on this issue.[34]

V. Effective Date

Many commenters noted that the proposed Guidance did not contain a delayed effective date. They suggested that the Agencies include a transition period to allow adequate time for financial institutions to implement the final Guidance.

The final Guidance is an interpretation of existing provisions in section 501(b) of the GLBA and the Security Guidelines. A delayed effective date is not required under the APA, 12 U.S.C. 553(d)(2), or the Riegle Community Development and Regulatory Improvement Act of 1994, 12 U.S.C. 4802, which requires a delayed effective date for new regulations, because the final Guidance is a statement of policy.

Given the comments received, the Agencies recognize that not every financial institution currently has a response program that is consistent with the final Guidance. The Agencies expect these institutions to implement the final Guidance as soon as possible. However, we appreciate that some institutions may need additional time to develop new compliance procedures, modify systems, and train staff in order to implement an adequate response program. The Agencies will take into account the good faith efforts made by each institution to develop a response program that is consistent with the final Guidance, together with all other relevant circumstances, when examining the adequacy of an institution's information security program.

VI. OTS Conforming and Technical Change

OTS is making a conforming, technical change to its Security Procedures Rule at 12 CFR 568.5. That regulation currently provides that savings associations and subsidiaries that are not functionally regulated must comply with the Security Guidelines in Appendix B to part 570. OTS is adding a sentence to make clear that Supplement A to Appendix B is intended as interpretive guidance only.

With regard to this rule change, OTS finds that there is good cause to dispense with prior notice and comment and with the 30-day delay of effective date mandated by the Administrative Procedure Act. 5 U.S.C. 553. OTS believes that these procedures are unnecessary and contrary to the public interest because the revision merely makes conforming and technical changes to an existing provision. A conforming and technical change is necessary to make clear that Supplement A to Appendix B to part 570 is intended as interpretive guidance only. Because the amendment in the rule is not substantive, it will not affect savings associations.

With regard to this rule change, OTS further finds that the Riegle Community Development and Regulatory Improvement Act of 1994 does not apply because the revision imposes no additional requirements and makes only a technical and conforming change to an existing regulation.

---

[31] *See* CAL. CIV. CODE § 1798.82(g)(3) (West 2005).

[32] Under the E-Sign Act, if a statute, regulation, or other rule of law *requires* that information be provided or made available to a consumer in writing, certain consent procedures apply. *See* 15 U.S.C. 7001(c).

[33] 47 CFR 64.1200.

[34] The Agencies note, however, that the TCPA and its implementing regulations generally exempt calls made to any person with whom the caller has an established business relationship at the time the call is made. *See, e.g.,* 47 CFR 64.1200(a)(1)(iv). Thus, the TCPA would not appear to prohibit a financial institution's telephone calls to its own customers. In addition, the FCC's regulations state that the phrase for ''emergency purposes'' means calls made necessary in any situation affecting the health and safety of consumers. 47 CFR 64.1200(f)(2). *See also* FCC Report and Order adopting rules and regulations implementing the TCPA, October 16, 1992, available at *http://www.fcc.gov/cgb/donotcall/,* paragraph 51 (calls from utilities to notify customers of service outages, and to warn customers of discontinuance of service are included within the exemption for emergencies). Financial institutions will give customer notice under the final Guidance for a public safety purpose, namely, to permit their customers to protect themselves where their sensitive information is likely to be misused, for example, to facilitate identity theft. Therefore, the Agencies believe that the exemption for emergency purposes likely would include customer notice that is provided by telephone using an artificial or prerecorded voice message call.